Golpes: Evite Fraudes

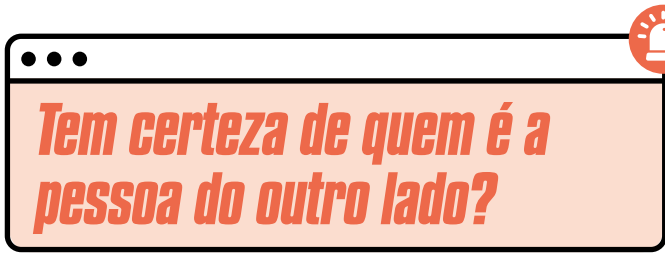
Produção:

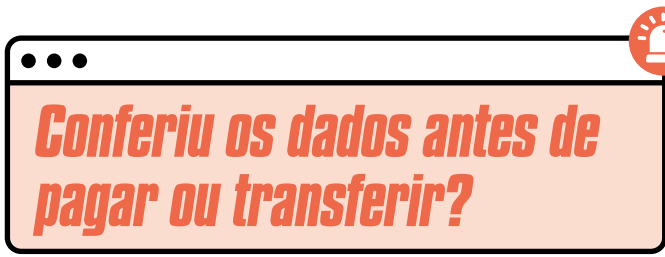
cert.br nic.br cgi.br

DESCONFIE. PREVINA-SE.

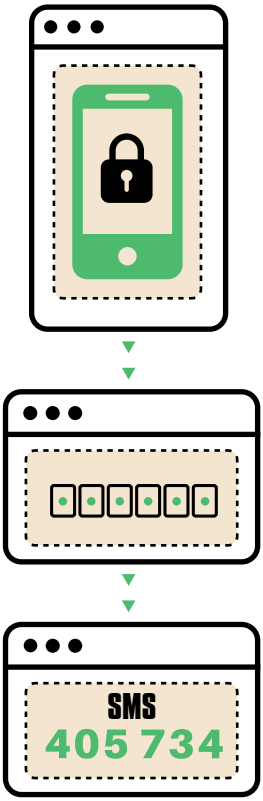
Além de manipular as emoções das pessoas, fraudadores também se aproveitam de brechas de segurança para aplicar golpes.

Veja aqui como se proteger.





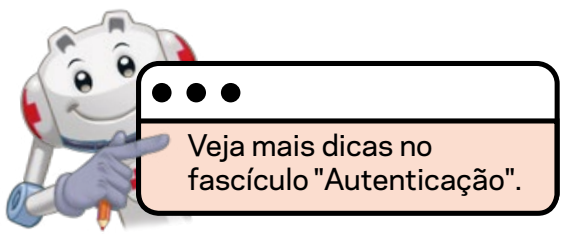
NA DÚVIDA, DIGA NÃO E DENUNCIE



PROTEJA SUAS CONTAS

Por que golpistas querem acessar suas contas? Para se passar por você, usar seus dados, gastar seu dinheiro, fazer dívidas em seu nome e enganar seus contatos.

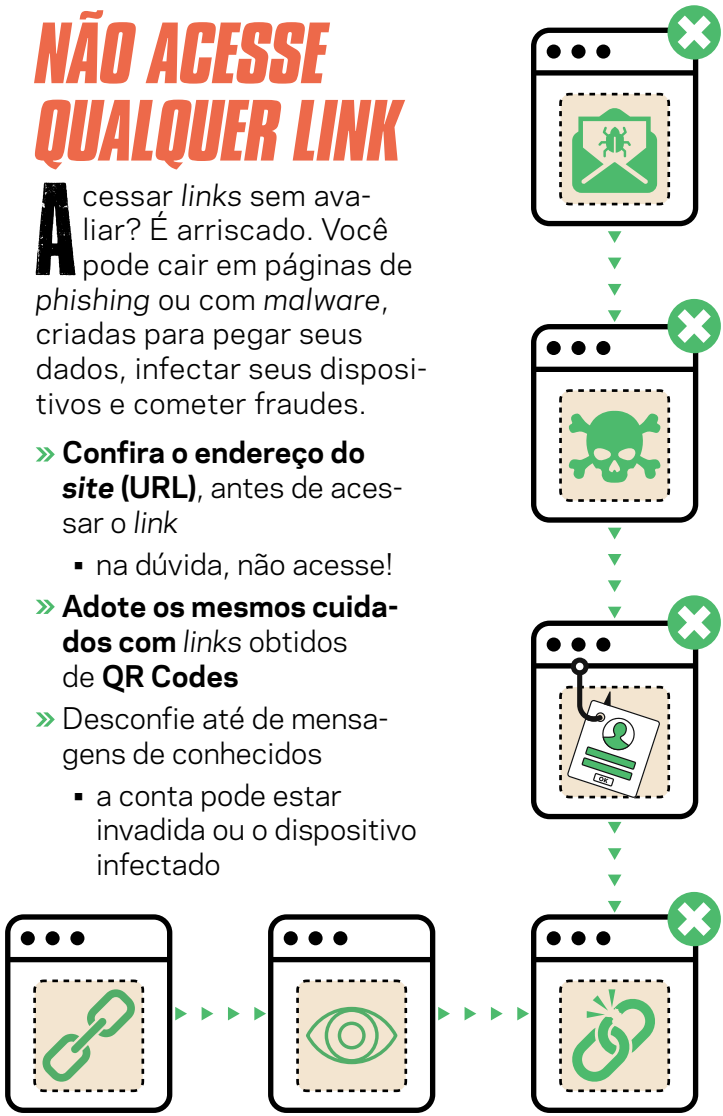
- Use senhas fortes
- **Ative a verificação em duas etapas**
- **Não passe** senhas nem códigos de verificação
- Redobre a atenção com contas importantes, como as usadas para:
  - **recuperar senhas**
  - **acessar vários serviços** (ex: gov.br)



NÃO ACESSE QUALQUER LINK

Acessar *links* sem avaliar? É arriscado. Você pode cair em páginas de *phishing* ou com *malware*, criadas para pegar seus dados, infectar seus dispositivos e cometer fraudes.

- **Confira o endereço do *site* (URL)**, antes de acessar o *link*
  - na dúvida, não acesse!
- **Adote os mesmos cuidados com** *links* obtidos de **QR Codes**
- Desconfie até de mensagens de conhecidos
  - a conta pode estar invadida ou o dispositivo infectado



Phishing é um **tipo de fraude** na qual golpistas tentam obter informações pessoais e financeiras, **combinando engenharia social com recursos técnicos**.

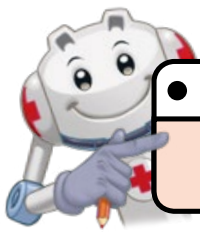
A palavra *phishing* vem do inglês "fishing", que significa "pesca". Os golpistas jogam "iscas" (mensagens) para tentar fisgar seus dados.

ACESSE SITES E APLICATIVOS OFICIAIS

Tem certeza de que o *site* ou *app* é autêntico? Todo cuidado é pouco. Golpistas criam páginas e *apps* falsos que imitam organizações conhecidas para fazer vítimas.

» Digite o endereço do *site* (URL) diretamente no navegador
  - **use conexões seguras** (https)
  - ao usar ferramentas de busca, **confira se a URL mostrada é a legítima**

» Instale *apps* só de **lojas oficiais**
  - antes de baixar, confirme se é o desenvolvedor correto
  - nunca use *link* ou *app* recebido por mensagem



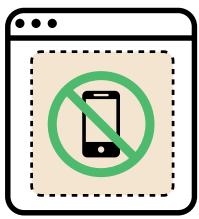
Veja mais dicas no fascículo "Celulares e *Tablets*".

BUSQUE O PERFIL OFICIAL

Quer fazer contato via rede social? Golpistas criam perfis falsos fingindo ser empresas ou pessoas conhecidas para pegar seus dados e pedir dinheiro.

» Antes de contatar um perfil, **confira se é o oficial**

- busque o nome do perfil na página oficial da empresa
- observe o histórico do perfil, como data de criação, publicações antigas e seguidores

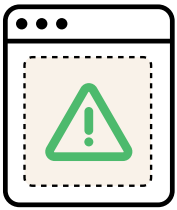


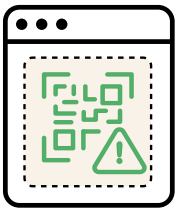
NÃO RESPONDA, DENUNCIE

Mensagem ou ligação com cara de golpe? Qualquer resposta pode **entregar informações** e colocá-lo em risco. **Denunciar ajuda a tirar do ar** anúncios e perfis falsos e evitar que outras pessoas caiam.

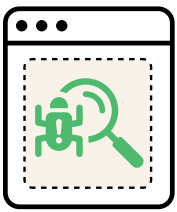
- Denuncie mensagens, anúncios e perfis maliciosos
  - use os recursos disponíveis nas plataformas
- **Bloqueie** telefones e contas que enviam mensagens suspeitas
- **Evite atender** chamadas de **números desconhecidos**
  - use filtros (ex: da operadora, do sistema do celular)

CUIDADO COM QR CODES EM LOCAIS PÚBLICOS

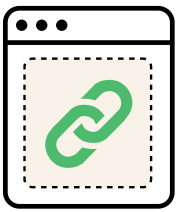


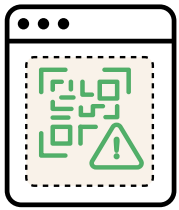


Vai ler QR Code em local público? Golpistas podem **substituir códigos originais por falsos** em placas, folhetos, cartazes, mesas, parquímetros e objetos de acesso coletivo.



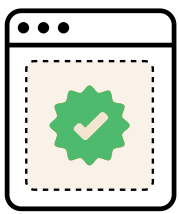
- **Evite** ler QR Codes de **fontes desconhecidas**
- Antes de ler o QR Code:
  - **procure sinais de alteração**
  - confira se não há adesivo colado por cima
- Redobre a atenção em restaurantes, estacionamentos, caixas eletrônicos, propagandas na rua e transportes públicos
- Na dúvida, não leia e **avise alguém responsável pelo local**





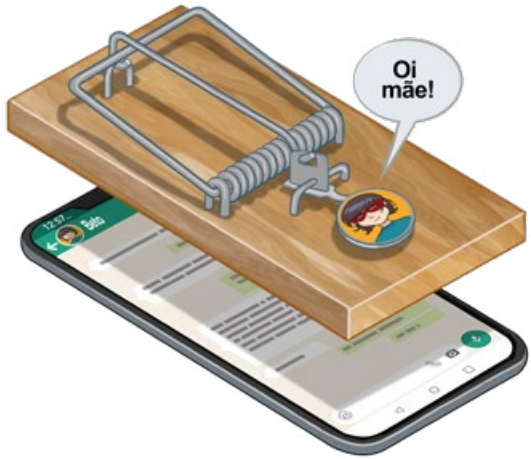
ANTES DE PAGAR, CONFIRA OS DADOS DO QR CODE

Sabia que golpistas usam QR Codes para furtar dinheiro? Eles trocam os códigos para **desviar o pagamento** para outra conta. Também mandam cobranças falsas por mensagens.



» Prefira ler ou copiar QR Codes **diretamente de *sites* e *apps* oficiais**
  - ignore QR Codes recebidos por mensagens

» **Antes de confirmar** pagamentos e transferências, observe:
  - o **valor** mostrado está certo?
  - os **dados de quem vai receber**, como CNPJ e nome, estão corretos?



CONFIRME PRIMEIRO, TRANSFIRA DEPOIS

A pessoa da **foto é conhecida**, mas o número do **telefone é diferente**? Desconfie! Golpistas usam fotos de redes sociais para enganar amigos e familiares.

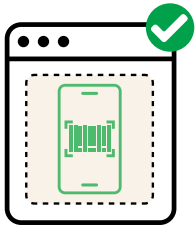
» Não acredite que a pessoa é quem diz ser
  - converse com a pessoa conhecida pelo **contato de sempre**
  - **não salve** o novo número **sem confirmar** antes

» Desconfie de **qualquer pedido de dinheiro**
  - mesmo que seja comum na família

» Antes de fazer transferências ou pagamentos, **confira os dados de quem vai receber**
  - na dúvida, não faça!

CONFIRA OS DADOS DE BOLETOS

Será que o boleto é verdadeiro? Golpistas enviam boletos falsos se passando por empresas conhecidas e, ao pagar, o dinheiro vai para a conta deles.



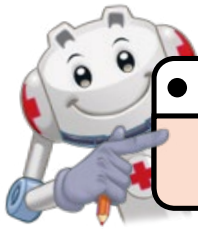
» **Antes de pagar**, pergunte-se:

- devo mesmo essa despesa?
- o valor cobrado está correto?
- os dados de quem vai receber, como nome e CNPJ, são do fornecedor que contratei?

» Prefira **boleto eletrônico registrado**

- o pagamento vai para o emissor registrado

» Em caso de dúvida, **contate o fornecedor via canais oficiais**



Veja mais dicas no fascículo "Banco via Internet".

SÓ DEVOLVA PIX PARA A CONTA DE ORIGEM

Recebeu Pix "por engano" e pediram que devolva para outra conta? Não caia nessa. Se o dinheiro não voltar para a conta de origem, o golpista pode pedir o estorno usando o Mecanismo Especial de Devolução (MED). No final, **você devolve duas vezes**.

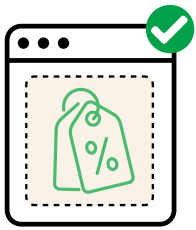
» Confirme no extrato se o Pix caiu mesmo

» Use a **opção de devolução** no *app* ou *site* do banco

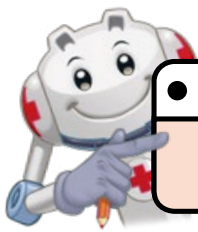
- **não faça um novo Pix**

VERIFIQUE SE O SITE OU VENDEDOR É CONFIÁVEL

Oferta imperdível? Melhor conferir! Golpistas criam *sites* falsos com preços muito abaixo do normal. Depois que você paga, eles somem e o produto não chega. E ainda podem usar seus dados em outros golpes.



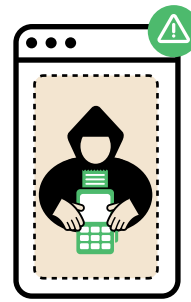
- Compare preços e **desconfie de ofertas boas demais**
- **Pesquise a reputação** em redes sociais, *sites* de reclamações e de defesa do consumidor
- Prefira *sites* e vendedores que você já conhece ou tenha boas referências



Veja mais dicas no fascículo "Comércio via Internet".

SÓ PAGUE NA PLATAFORMA ORIGINAL DA COMPRA

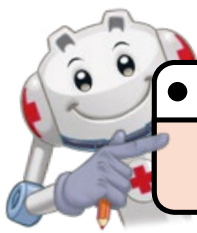
Fez uma compra e estão pedindo taxa extra por outro canal? Cuidado com o golpe! Além de você pagar a mais, podem clonar seu cartão e usar seus dados em fraudes. Sem falar que você pode virar um "alvo preferido".



» Na dúvida, **contate a plataforma por canais oficiais**

» Ao fazer qualquer pagamento:

- no Pix ou boleto, **verifique os dados do recebedor**
- **confira o valor antes de autorizar** a cobrança
- **confirme o valor cobrado** em sua conta ou cartão



Veja mais dicas no fascículo "Comércio via Internet".

EVITE QUE ABRAM CONTAS BANCÁRIAS COM SEU CPF

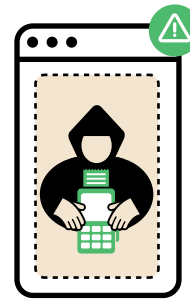
Apareceu uma despesa que você não fez? Seu nome ficou sujo na praça? Fraudadores usam dados vazados para abrir contas bancárias, fazer empréstimos e movimentar dinheiro de outras vítimas.

» **Ative a proteção BC PROTEGE+** do Banco Central **https://www.bcb.gov.br/meubc/bcprotege/**

» Desative **temporariamente** a proteção quando precisar

- agende a **reativação automática**

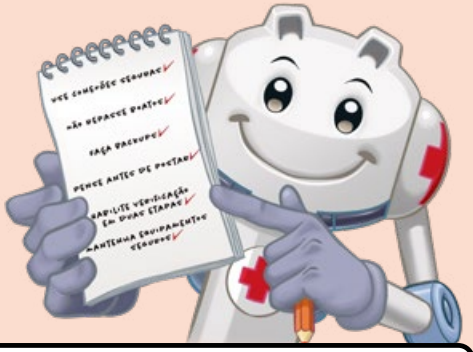
BLOQUEIE A ABERTURA DE EMPRESAS COM SEU CPF



Já imaginou seu nome envolvido com empresas fantasmas e golpes? Fraudadores podem usar seu CPF para abrir empresas falsas e usá-las em golpes ou operações ilegais, como lavagem de dinheiro.

» **Ative a Proteção do CPF** no Portal Nacional da Redesim **https://www.gov.br/empresas-e-negocios/pt-br/redesim/**

Veja mais sobre golpes e fraudes nos Fascículos "**Golpes: Não se Deixe Enganar**" e "**Golpes: Caiu? Veja o que Fazer**".



SAIBA MAIS

- Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança para Internet, disponíveis em: **https://cartilha.cert.br/**
- Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores, confira em: **https://internetsegura.br/**

cert.br

O CERT.br **(https://cert.br/)** é um Grupo de Resposta a Incidentes de Segurança (CSIRT) de responsabilidade nacional de último recurso, mantido pelo NIC.br. Além da gestão de incidentes, também atua na conscientização sobre os problemas de segurança, na consciência situacional e transferência de conhecimento, sempre respaldado por forte integração com as comunidades nacional e internacional de CSIRTs.

nic.br

O Núcleo de Informação e Coordenação do Ponto BR - NIC.br **(https://nic.br/)** é uma entidade civil de direito privado e sem fins de lucro, encarregada da operação do domínio .br, bem como da distribuição de números IP e do registro de Sistemas Autônomos no País. Conduz ações e projetos que trazem benefícios à infraestrutura da Internet no Brasil.

cgi.br

O Comitê Gestor da Internet no Brasil **(https://cgi.br/)**, responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados.

https://cartilha.cert.br/cc/

março / 2026